Which?
2 Marylebone Road
London NW1 4DF
020 7770 7000
which.co.uk

6 October 2026

Consultation response

Which? response to HM Treasury consultation on modernising payment services regulation

We welcome the opportunity to respond to HMT's consultation on modernising payment services regulation to ensure that payments continue to work well for consumers. Our recommendations are grouped into the three broad areas set out in the consultation:

Modernising the Regulatory Framework

- **Retain core consumer rights in law:** We support modernising payments regulations so they remain appropriate for consumers' needs. We agree that having some details of payments regulation in Financial Conduct Authority (FCA) rules has the potential to offer greater flexibility on points that are uncontentious. However, as HM Treasury itself recognises, core perimeter definitions and fundamental consumer rights must remain preserved in legislation to prevent hard legal remedies from being reduced to discretionary supervisory oversight. Our response provides a list of some key provisions from the Payment Services Regulations 2017 (PSRs) which must be retained in statute.
- **Assess each provision proposed for transfer to FCA rules so there is no diminution in consumer protection:** While modernising regulations and shifting routine administrative rules to FCA rules can offer flexibility, each provision proposed for transfer must be carefully evaluated to ensure that the transfer does not result in a reduction in consumer protection.
- **Redefine authorisation for payments:** HMT should update the legal definition of payment authorisation so entering security codes is not automatically treated as irrefutable proof of legal consent, ensuring victims of fraud and social engineering scams are not left without protection and can still get their money back.
- **Guarantee support for non-digital and vulnerable users:** Legislation should guarantee access to support channels (e.g. branch services), require Payment Service Providers (PSPs) to implement a secure, standardised digital delegation tool to allow consumers to grant trusted third parties (e.g. carers) limited access to their account, and ensure all payment methods offer a consistent level of purchase protections.
- **Regulate digital wallets and expand 'payment account' definition:** Digital wallets like Apple Pay and Google Wallet should be brought under FCA oversight to close liability and operational risks. In addition, the statutory definition of a 'payment account' should be expanded to include instant-access savings and Cash ISAs, broadening Open Banking and advancing Open Finance by giving consumers a more complete picture of their savings and making it easier for them to automatically move excess funds into accounts offering higher rates of interest

Responding to New Developments in Payment Services

- **Give clear and equal protections for users of new forms of payments:** Technological innovation in payments must not come at the expense of consumer protection. We welcome HM Treasury's 'same risk, same regulatory outcome' principle to guide the development of new payment services. As part of this approach, HMT must ensure tokenised bank deposits offer protections like FSCS cover, enforce strict product labels to stop crypto assets or stablecoins from being mis-sold as savings, and mandate that all digital payment rails (including Open Banking account-to-account payments) offer baseline dispute and refund standards.
- **Apply strict checks to firms seeking to offer new types of payments and ensure they adequately safeguard consumers' money:** Existing payment firms must not be allowed to roll out tokenised payments or stablecoins under old permissions. The FCA must carefully check each firm, reviewing their governance and processes for security and fraud prevention. In addition, consumers' money must be ring-fenced to protect customers if a firm fails.
- **Implement safeguards for agentic payments:** As AI agents able to make payments go live, regulations must adapt to protect consumers from risks such as unauthorised or incorrect purchases, and unfair liability shifts. While voluntary industry initiatives like agent registries and single-use virtual cards are welcome, they are not enough on their own. To stop providers from shifting system risks onto users and keep pace with fast-moving innovation, HMT must establish a statutory baseline requiring secure verification of AI agents, clear provider liability for execution errors, traceable decision logs, and granular, easily revocable consumer controls.
- **Build resilient networks:** There are two major areas that the Government should address that are not dealt with in HMT's consultation: future-proofing payment security against quantum computing, and ensuring resilience when digital networks fail by exploring offline payments and safeguarding access to cash.
- **Hold senior executives accountable to raise governance standards:** The Senior Managers & Certification Regime (SM&CR) should be extended to payment and e-money firms so executives are held personally responsible for fixing governance failures and preventing financial crime.

Unlocking the Future of Open Banking

- **Mandate statutory expansion and universal participation:** Transition Open Banking to a permanent statutory framework under the FCA, empowering the regulator to mandate universal bank participation and keep basic APIs free of charge to protect competition. Relying on voluntary participation would render account-to-account payments patchy and unreliable for both consumers and merchants.
- **Enforce consumer controls for VRPs and sweeping:** Ensure advanced features like Variable Recurring Payments (VRPs) and fee-free sweeping feature strong protections, including standardized and simple mechanisms to revoke consent and robust dispute standards.
- **Ensure robust oversight and data trust:** Embed a mandatory Smart Data Trust Framework centered on cybersecurity, data minimisation, inclusive design, and protections against misuse such as data exploitation, dark patterns, and predatory profiling.

ANSWERS TO QUESTIONS

Chapter 1 questions

Question 1: Which firm facing requirements should remain in legislation and which should be delegated to the FCA? Please explain your reasoning.

We support modernising payments regulation in whatever way is most appropriate for consumers' needs, including their protection where necessary. We also agree that having some details of payments regulation in FCA rules has the potential to offer greater flexibility on points that are uncontentious so that legislative scrutiny may not be required. However, moving detailed rules into the FCA Handbook raises three fundamental concerns:

1. **Erosion of statutory legal rights:** Moving protections from statute to regulatory rules strips consumers of their direct right of action in court. Under the current PSRs, consumers can bring legal claims under regulation 148 for breaches of requirements. More generally, breaching an FCA rule does not automatically grant a civil cause of action unless explicitly preserved under Section 138D of FSMA 2000. Where rights are delegated, legislation must confirm that consumers retain this direct right of legal action.
2. **Limitations of Ombudsman redress:** Transferring statutory rights to FCA rules leaves the Financial Ombudsman Service (FOS) as the primary avenue for redress. While vital, FOS decisions do not set binding legal precedents, are subject to compensation caps, and current proposed Government reforms risk further eroding consumer access to fair, timely dispute resolution.
3. **Gaps in regulatory enforcement:** The FCA focuses on systemic, market-wide supervision rather than individual claims, and in general does not award restitution for individual consumers subject to rule breaches. This means enforcement is often slow, occurs only long after consumer harm has occurred, and does not compensate consumers.

Any such moves to shift legislative provisions into FCA rules must therefore be very carefully considered. Rather than adopting a sweeping approach to reform, each individual legislative requirement set out in the Payment Services Regulations 2017 (PSRs) and the Electronic Money Regulations 2011 (EMRs) that is considered for transfer to FCA rules must be evaluated and a rationale provided for the move, along with a clear explanation of how such a move will not result in any reduction in consumer rights or protections, including in relation to how they may be enforced.

Not all of the requirements should be transferred. A range of organisations - including Which? - have previously raised concerns about removing or diluting consumer protections in financial services regulation, for example in the Future Regulatory Framework review, the passing of the Financial Services and Markets Act 2023, and reform of Consumer Credit Act 1974 consultations and proposals for reform. HM Treasury has not always taken account of such concerns. Yet as HM Treasury recognises in relation to payments regulation, an appropriate balance must be struck: essential elements, core perimeter definitions, and fundamental consumer rights must remain preserved in legislation to maintain predictable statutory certainty and clarity.It is essential HMT sticks to this approach. Delegating key rights to regulator rules

risks converting hard legal remedies into discretionary supervisory oversight, which we firmly oppose.

What must remain anchored in legislation

The following is a list of key provisions from the PSRs which must be retained in legislation:

1. Core Fraud & Liability Protections

- **Consent and withdrawal of consent (Regulation 67):** Defines the foundational legal baseline that a transaction is only authorised if explicit consent is given, including in relation to consent for continuous payments, and helps to prevent firms from shifting the financial burden of sophisticated fraud onto consumers. Retaining this important right in statutory law ensures it cannot be diluted without Parliamentary approval.
- **Notification and rectification of unauthorised or incorrectly executed payment transactions (Regulation 73):** Establishes the 13-month statutory long-stop limitation window for consumers to notify PSPs of unauthorised payments, providing a clear baseline that is helpful for consumers, their advisers and firms.
- **Evidence on authentication and execution of payment transactions (Regulation 75):** Places the legal burden of proof on the PSP to prove that a transaction was authenticated, correctly recorded, and entered into the accounts. Retaining this in statute takes the information / power asymmetry into account and ensures PSPs keep the obligation to provide evidence.
- **Payment service provider's liability for unauthorised payment transactions & Requests for refund for payee-initiated transactions (Regulations 76 & 79):** The obligation for PSPs to refund unauthorised transactions by the end of the next business day provides an immediate, enforceable statutory right. Keeping this in legislation retains a clear, strict liability and ensures a consistent approach. Delegating this to FCA rules risks converting enforceable legal rights into vague guidelines, potentially exposing consumers to prolonged financial distress while disputes are dealt with via bureaucratic channels.
- **Payer's liability for unauthorised payment transaction (Regulation 77):** The £35 liability cap for losses serves as a critical safety net for consumers, limiting their exposure to losses.

2. Execution Certainty & Settlement Rules

- **Payment transactions to a payment account, Amounts transferred, and Defective execution (Regulations 86, 89 & 91):** Statutory requirements regarding D+1 settlement timelines (Reg 86), full amount delivery without unauthorized fee deductions (Reg 89), and PSP liability for late or defective execution (Reg 91) ensure retail settlement certainty. Delegating this could invite reductions to execution speed or the addition of hidden processing fees.

3. Contractual Fairness & Transparency

- **Information for the payer after receipt of payment order & Information for the payer after execution of individual payment transactions (Regulations 45 & 53):** Statutory mandates for post-transaction information guarantee consumers access to clear transaction references and payment details. Maintaining this in legislation provides

helpful clarity for consumers and prevents PSPs from obscuring statement data or reducing disclosure under flexible regulatory rules.

- **Changes in contractual information & termination of framework contract (Regulations 50 & 51):** Statutory mandates ensuring free-of-charge contract termination and a mandatory advance notice period for changes made by PSPs are essential to allow consumers to easily switch and provide protection against surprise fee hikes.
- **Burden of proof on payment service provider (Regulation 59):** Obligates the PSP to prove that it met its pre- and post-contractual disclosure duties. Keeping this in statute preserves a binding legal presumption in favor of consumers during disputes, and helps to partially mitigate knowledge and information asymmetries.

4. Financial Inclusion & Competition

- **Access to payment systems & Access to payment account services (Regulations 102–104):** Legislative access rights protect consumers against unfair "de-banking" and mandate non-discriminatory account access for third-party providers. Access to payment services is essential to participate in modern society, and so it is for Parliament to set this baseline to prevent PSPs from denying consumers access to payment accounts.

5. Redress via legal system

- **Right of action (Regulation 148):** Creates an explicit statutory right for private individuals to seek court damages for a PSP's breach of duties. Removing this to FCA rules risks stripping consumers of access to justice, leaving them dependent on regulatory enforcement or ombudsman remedies. The existence of this right will be an important deterrent factor for PSPs when individual consumers allege with justification that their rights have been breached.

Question 2: Where you believe requirements should remain in legislation, are there any updates you believe need to be made to these requirements?

Yes. We believe that activity to modernise and future-proof the legislative framework for the regulation of payment services should include updating areas where the existing rules fall short or need to be adapted to address emerging risks. We suggest several legislative updates to ensure statutory protections remain fit for purpose:

1. **Redefining 'Authorised Payment':** The current legislative approach treats all payments as either authorised or unauthorised, relying on technical authentication (delivered via SCA) as definitive proof of authorisation. This approach is obsolete since it assumes that inputting valid credentials equals informed intent, ignoring increasing levels of social engineering and sophisticated manipulation.

   Published Ombudsman decisions involving consumers (e.g. DRN-5461457 and DRN-4949831) demonstrate how Regulation 67 of the PSRs 2017 binds the FOS to a mechanical definition of consent. In DRN-5461457, the Ombudsman explicitly ruled that *"for the purposes of whether a payment is authorised, it doesn't matter if [the consumer] was deceived about the purpose or amount of the payment*". In DRN-4949831 the Ombudsman stated *"The fact she understood, by completing the steps she did, that payments would be leaving her account is enough to say, under the PSRs, they were authorised by her. I recognise they didn't go to a new, safe bank account as she*

intended, but this isn't part of the test." Because the PSRs tie authorisation strictly to credential execution rather than intent, the Ombudsman must treat social-engineered payments as authorised.

We suggest HM Treasury addresses this structural flaw by amending the statutory definition of an "authorised transaction" to clarify that technical authentication provides only a *presumption* of consent. This definition can be invalidated where consent was obtained through deception, impersonation, or coercion, shifting the evidentiary burden onto the PSP to prove gross negligence rather than forcing the consumer to disprove their own authorisation.

Such a move would ensure UK consumer protections do not fall behind international standards. Article 55(2) of the proposed EU Payment Services Regulation (PSR) establishes that technical authentication alone does not prove legal authorization. It states:

> *"Where a payment service user denies having authorised an executed payment transaction, the fact that the payment transaction was authenticated, including where applicable, via strong customer authentication, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52. The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user."*

In taking forward work in this area, HMT should ensure alignment with work being carried out by the Home Office on unauthorised fraud.

2. **Non-digital service baseline:** As payment infrastructure shifts to online and digital channels making use of biometrics and smartphones, we risk excluding those who cannot access these technologies. Legislation should include explicit duties requiring firms to maintain accessible, non-digital channels (e.g. telephone or physical branch access) for essential tasks, including dealing with suspected fraud and dispute resolution. This is strongly reinforced by the FCA's report on Payments firms: delivering good outcomes for consumers in vulnerable circumstances (September 2026), which warns that pure digital or transactional business models "amplify the potential for harm" due to limited human contact when issues arise.

3. **Delegated digital access framework:** The current legislative framework forces millions of vulnerable consumers to adopt high-risk workarounds, such as sharing banking passwords or PINs with carers, which leaves them open to abuse and voids fraud liability protections. Legislation should require PSPs to implement a secure, standardised digital delegation tool. This tool must allow account holders to grant trusted third parties (e.g. carers) flexible and granular permissions (e.g. "pay utility bill X up to £Y each month") without requiring the sharing of full credentials or account control. We cover this in more detail in our answer to Question 17.

4. **Baseline for payment purchase protections:** As new payment methods emerge, we are witnessing a dangerous 'protection gap' emerge. Current consumer purchase protection rights - such as those under Section 75 of the Consumer Credit Act or chargeback - are tied to specific payment methods, leaving consumers unknowingly unprotected when they use newer retail payment rails such as Open Banking account-to-account payments. The PSR has suggested that it supports a market-driven approach to providing and improving consumer protection in account-to-account payments, dating back to its Policy Statement on Consumer protection in interbank payments (October 2021). While we welcome industry efforts to grapple with this issue (e.g. UK Finance proposals for cVRP protections), little progress has been made. Legislation should mandate that all digital payment transactions must incorporate a baseline dispute and refund standard. This would help to give consumers the confidence to try new and emerging digital payment methods like cVRPs, encouraging innovation and competition.

5. **Consider extending the regulatory perimeter to digital wallets[1]:** Digital wallets are an increasingly integral feature of the UK's payments landscape and have become a popular way for consumers to pay - UK Finance report that in 2025, approximately 37.6 million consumers, more than six in ten in the adult population, were registered to use at least one mobile wallet service and 58% used mobile payments to purchase goods or services at least once a month. The rapid rise of digital wallets has created a regulatory gap. Under current rules, pass-through wallets (e.g. Apple Pay, Google Wallet) are classified as unregulated Technical Service Providers (TSPs), while staged/stored-value wallets (e.g. PayPal) are fully regulated. This distinction is confusing to consumers and leads to risks around:

    - **misaligned liability to combat fraud:** PSPs bear sole statutory liability for unauthorised transactions, even though digital wallet providers control device biometrics (Face ID/Touch ID) and tokenisation interfaces.
    - **redress and resolution gaps:** Consumers have no legal recourse via the FOS against wallet operators for problems which may arise such as interface glitches, software outages, or token handling errors.
    - **unregulated operational risk:** more than six in ten in the adult population are registered to use a mobile wallet service, meaning they represent a major potential risk if they were to suffer some form of outage, yet they currently sit outside FCA oversight.

    As it seeks to modernise the payments framework, HM Treasury should consider bringing digital wallet providers within the regulatory perimeter, subjecting them to direct FCA oversight, and making them subject to the Consumer Duty and operational resilience requirements.

6. **Closing potential loopholes when changing or terminating contracts:** In our answer to Q1 we made the case for retention in legislation of changes in contractual information & termination of framework contract (Regulations 50 & 51). However, retention in

[1] As in the new Australian legislation, see https://www.legislation.gov.au/C2025A00046/asmade/text.

legislation alone is not sufficient. As we have seen with the application of comparable rules under Ofcom's regime, firms can side-step statutory exit rights by embedding pre-agreed fee escalators or variable pricing formulas into initial terms. HMT should update statutory drafting to close these contractual workarounds.

Question 3: Do current provisions relating to the regulatory framework for payment services and electronic money, such as key definitions, need to be updated? If so, please explain how.

Yes. To ensure the framework supports financial innovation and consumer protection, we propose two fundamental updates to the statutory definitions:

1. **Expand the Definition of 'Payment Account'.** The current definition of a 'payment account' is narrow, excluding the vast majority of instant-access savings accounts and Cash ISAs because they require an intermediate transfer to a "nominated" current account. We recommend that HM Treasury expand the statutory definition to include instant-access savings products. By bringing these accounts under the payment account definition, they would become eligible for Open Banking API access without having to wait for sector-specific secondary legislation. This would fast-track part of the Government's aspiration to embrace Open Finance. Doing so would provide a range of benefits to consumers at an earlier stage than would otherwise be the case: they would gain a view of all their payments and savings accounts in one place, and be able to use open banking's sweeping functionality to automatically move excess funds from low-interest accounts into high-yield products. This would help efforts to tackle the loyalty penalty and incentivise competition between savings account providers.
2. **Clarifying consent as explicit and purpose-bound -** The current legislative definition of "consent" is too binary and lacks the detail and nuance that will be required for expansion of Open Banking and moves towards agentic payments. We suggest HMT consider amending the statute to define consent as:
    - **Explicit and purpose-bound:** Consent must be defined as an active, time-limited, and purpose-restricted authorization. It must be legally established that granting access for a specific service (e.g. 'account aggregation') does not constitute implied consent for other services (e.g. 'onward data-sharing with third-party marketing affiliates').
    - **Revocable:** The definition must include a 'Right to Revocation' to ensure that the withdrawal of consent is technically, legally and practically as simple as the granting of consent.

Question 4: Which international regulatory developments, for example recent reforms in the EU, should the UK incorporate into an updated framework for payment services and electronic money?

As we set out in our answer to Question 2, we think HM Treasury should reflect the approach adopted in the EU's Third Payment Services Directive (PSD3) and Payment Services Regulation (PSR) regarding the legal treatment of 'authorisation' and consumer liability.

The EU framework establishes that successful Strong Customer Authentication (SCA) is not, in itself, sufficient proof of valid user consent. We should adopt a similar approach that technical

security logs provide only a *presumption* of consent, which can be invalidated if it is proven that the user was subjected to manipulation, social engineering, or coercion. This would help to ensure that the FOS and the courts are no longer legally bound to treat manipulated credential entry as a "valid instruction."

The government should also consider consolidating APP fraud protection into the core legislative requirements for payments regulation, as is proposed (and agreed subject to final adoption) in the EU.

Chapter 3 questions - Responding to new developments in payment services

Summary of our approach

Our primary concern is that technological innovation in payments must not come at the expense of consumer protection. We welcome HM Treasury's 'same risk, same regulatory outcome' principle to guide the development of the regulatory framework that will apply to new payment services.

Rather than answering each question in this section individually, our response groups our answers to Questions 5-14 into three areas which focus on core consumer priorities: ensuring the same levels of protection, robust gatekeeping and safeguarding, and ensuring consumer control over programmable payments.

Priority 1: Same level of protection (Questions 5, 6, 9, 10)
We recognise that tokenised deposits have potential to offer consumers certain benefits such as programmability, and note early moves to test such transactions. Our stance is that consumers must have the same protections whether their payment travels over traditional bank rails or new blockchain technology. This should include:

- **Full protection for tokenised deposits:** If a bank tokenises a customer deposit, it remains a deposit. It must keep full statutory Financial Services Compensation Scheme (FSCS) protection up to £85,000 and access to the Financial Ombudsman Service (FOS).
- **Clear labels to prevent mis-selling:** Firms must provide clear information to consumers to accurately convey information about the safety of their money. Regulators must enforce strict naming rules, ensuring that non-bank stablecoins and e-money are not marketed as 'deposits' or 'savings', while standardised warnings must clearly state when money is not covered by the FSCS.

Priority 2: Robust gatekeeping and safeguarding (Questions 7, 8, 11)
New technology cannot mean light-touch supervision. Customer funds must be ring-fenced and returned quickly if a firm fails.

- **No automatic approvals (mandatory Variation of Permission):** Existing payment firms must not be allowed to roll out tokenised payments or stablecoins under old permissions. The FCA must check each firm first, specifically reviewing their governance arrangements, and processes for cyber security, fraud monitoring, and resilience.

- **Protection of customer money:** Stablecoin reserve funds must be kept separate from the company's own funds. If a firm goes bust, customer money must be protected from creditors, and returned quickly.

Priority 3: Ensuring consumer control over programmable payments (Question 12)
Automated payments must remain under the consumer's control. Many of the same considerations in relation to the issues raised by agentic payments (which we cover in response to Question 15 below) are also applicable to programmable payments, including the need for:

- **Clear, granular consent:** 'Smart contracts' or automated payment rules can lock up money or trigger automatic deductions. Firms must explain the implications of such arrangements to customers in simple, plain-English, and obtain clear permissions before setting up any automated payment rule.
- **Easily revocable:** Customers must have an easy, free, real-time way to cancel automated payment instructions or unlock their funds instantly through their banking app or customer service team.
- **Firm liability for technical glitches:** If programmable payments fail, the payment provider must bear full liability, and consumers must be refunded immediately for the costs of any missed payments.

Question 15: How does existing payment services regulation need to adapt to support agentic payments? For example, do provisions relating to authentication and consent of payments transactions, and liability for unauthorised payment transactions, need updating?

Current payment regulation will need changes to adapt to agentic payments. Existing payment frameworks are set up on the assumption of human involvement / approval, so are not well-aligned to delegated or autonomous agent execution.

As highlighted in the Mills Review, AI in retail financial services operates along an 'autonomy spectrum' which runs through five different roles. Current payment regulations can cope with the lower end of this spectrum, where AI is used as a tool but it is consumers who are required to make decisions (such as clicking 'confirm' when making a purchase). But agentic payments have the potential to push us to the far end of the spectrum, where consumers become 'observers' delegating continuous execution to AI software.

As payments move along this spectrum, several core steps in today's standard payment journey potentially break down because they depend on real-time human presence:

- **checkout review and confirmation:** no human is present to review terms or click 'pay now' to confirm the purchase.
- **real-time authentication:** security prompts required by SCA, like push notifications or SMS passcodes, will not work and time out when an agent acts autonomously in the background.
- **anti-fraud systems:** fraud engines tend to treat non-human activity as malicious attacks so would potentially block legitimate consumer AI agents.

- **binary dispute rules:** chargeback systems treat payments in binary way, categorising them as authorised or unauthorised, leaving them struggling to resolve cases where an agent may have made an error.

We have identified a number of core requirements to ensure agentic payments can operate safely for consumers which HM Treasury should take into account:

1. **Identity & authorisation verification**. For agentic payments to be secure, and to reduce risks of fraud or unwanted outcomes for consumers, payment firms must verify essential information about the agent such as its identity, ownership, and permissions:
    a. Verification of agent - The UK should put in place a framework under which firms can quickly and reliably establish AI agents as recognised entities when they try to carry out a payment. Such mechanisms should aim to confirm an agent is known, legitimate and trustworthy (not a fraudulent actor) and check the identity of the associated human. This would be an equivalent replacement of current SCA checks, which are designed with human users in mind, and should be the foundational layer of any payments-specific 'Know Your Agent' scheme that is developed.
    b. Verification of mandate - There must be clear processes to check that agents have been authorised by consumers and that the agent is operating within the parameters set by the consumer. At a basic level, this could rely on requiring the customer to provide payment confirmation each time a transaction is initiated by the agent. However, for ease of use and to deliver benefits offered by agentic payments, the consumer should be able to pre-authorise transactions within certain parameters (e.g. setting time limits, permissions only for specific businesses, and payment limits), including for multiple/recurring payments. In this scenario, PSPs must carry out robust automatic checks that an agent's payment request is within the mandate it has been given by the consumer. If the payment appears to be within the set boundaries it could go through without the consumer's input. If this is in doubt, the consumer could receive a notification or request to confirm. There should also be guidelines around the mandates set by the user, to ensure that they are always bounded, clear and easily revocable.

2. **Liability.** A clear liability framework is essential for consumer protection and redress. As AI becomes more autonomous, attributing responsibility for outcomes becomes more complex; it may not always be clear why an agent made a decision to execute a particular payment, or whether a payment should be classified as authorised or unauthorised. In addition, AI supply chains tend to be made up of many parties, complicating efforts to assign liability. Ensuring clear liability, and clarity around areas like disputes and chargebacks, is likely to require the setting of defined dispute resolution processes for agentic transactions, specific articulation of how chargeback rules apply, and regulator guidance on updates to payment firms' terms of service. If consumers are not appropriately protected, trust and confidence in agentic payments will be low, with knock-on consequences for efforts to realise benefits.

    This is already a live issue in the UK. For example, Instinct AI is currently undertaking its Beta phase testing that is available through invite-only in the UK. Its current online terms and conditions raise some points of concern. Instinct's terms allow the service to take "Actions" on a consumer's behalf and enter into agreements, commitments or transactions

that bind them, while also stating that the service is “not error-free”, that Actions “may not always be reversible”, and that Instinct is “not responsible for any unintended Actions or any loss, damage, charge, liability, or other consequence arising from Actions”. This raises a fundamental question about whether it is reasonable for consumers to bear potentially significant financial and legal consequences where those consequences arise from errors made by a system designed and controlled by the provider.

These concerns are heightened by the fact that Instinct also warns that safeguards may not prevent erroneous Actions and that “Records of Actions available through the Services may not always be accurate”, while placing responsibility on consumers to verify and monitor what the agent has done. This sits uneasily with established UK consumer protection principles. Under the Consumer Rights Act 2015, terms may be unfair where they create a significant imbalance in the parties’ rights and obligations to the detriment of the consumer, and firms cannot simply contract out of their obligation to provide services with reasonable care and skill. The fact that a provider designates an AI system as acting “on behalf of” the consumer should not, in itself, be sufficient to transfer the consequences of failures in that system onto the consumer.

As agentic AI develops, Government and regulators should act swiftly to ensure that liability reflects where meaningful control and responsibility actually sit. There is an important distinction between a consumer being responsible for the instruction they provide and being responsible for an agent incorrectly executing that instruction. Providers should not be able to capture the benefits of increasingly autonomous services while shifting the risks of erroneous or unintended actions almost entirely onto users. A clear principle is needed that consumers should not be left financially or legally disadvantaged by failures in agentic systems that they could not reasonably foresee, prevent or correct.

In terms of specific payments-related risks, recent launches and beta testing of consumer AI shopping agents - such as Instinct - have highlighted serious issues, such as agents accessing and exposing sensitive payment details, like credit card numbers and passwords. While we welcome proactive industry innovations such as Visa, Mastercard and Ant International introducing agent registries and Know Your Agent (KYA) protocols, and Stripe providing single-use virtual cards with spending limits to address some of these risks, voluntary commercial solutions are not enough. A fragmented, market-led approach leaves critical protection gaps which many consumers will not be aware of. Government and regulators should move swiftly to ensure consistent standards for agentic payments and enshrine liability protections and verifiable intent mechanisms so that consumers do not bear the financial burden of errors when payments are made via agents. Ultimately, ensuring consumers can have full confidence in these mechanisms means they will be far more likely to embrace and trust emerging agentic payments.

3. **Monitoring.** Firms should implement continuous monitoring to ensure agents always operate within their parameters, especially as mandates may change over time. One-off verification will not be enough. In addition, firms should implement monitoring systems for agentic payments that can flag unusual activities by agents that could indicate e.g. fraud risks.

4. **Supervision**. It is essential for regulations to enable effective supervision of agentic payments. Agent providers and payments firms should be required to maintain traceable, easy-to-read decision logs showing the mandate, verification checks made, the external data relied upon, and the logic used to make the payment. These records should be accessible to consumers on request in order to support redress rights and processes.

5. **Data quality, technology and systemic risk** Safe agentic payments require robust underlying infrastructure, interoperability, and proactive risk management:
    a. *Data/tech needs* - AI agents rely on high quality data feeds. Ensuring that the data necessary for agents to make payments is of high quality and reliable is essential.
    b. *Open standards and interoperability* - the use of open standards should be prioritised so AI agents making payments are able to interact with other AI tools and agents, non-AI tools, and wider data, to enable broader agentic finance.
    c. *Risk management* - regulators must guard against over-reliance on particular parties within the AI supply chain, if consumers or payments firms are utilising the same providers to enable agentic technology.
    d. *Financial inclusion* - payments firms should ensure the agentic payments they enable can operate in a straightforward way using simple information and interfaces that consumers will understand, to reduce exclusion of any consumer groups.

Question 16: Are there any other innovations across the payments landscape that the Government should take into account when reforming its payment services regulatory framework?

There are two major areas that the Government should consider that are not dealt with elsewhere in HMT's consultation: future-proofing payment security against quantum computing, and ensuring everyday spending resilience when digital networks fail.

Quantum computing: preparing payments infrastructure for risks. Current payment regulations assume that today's standard encryption methods will remain secure indefinitely. However, the rapid advancement of quantum computing is likely to give criminals the capability to break the mathematical locks that currently protect online banking, digital wallets, and Open Banking API connections. The Mills Review into AI and the future of retail financial services explicitly identified quantum computing as a major "disruptive uncertainty" with systemic consequences for financial infrastructure.

While the timeline for quantum maturity remains uncertain, the threat to financial data and payment security is reportedly already occurring. We understand that criminals are capturing and storing encrypted payment streams and transaction histories today - a tactic known as "Harvest Now, Decrypt Later" - so they can be unlocked once quantum computing matures, exposing years of sensitive consumer spending habits, locations, and personal credentials. In addition, it is anticipated that quantum tools will eventually make it possible to forge the digital signatures used to authenticate payments, creating a severe risk that consumers could be wrongly blamed for fraudulent activity if security protocols can no longer reliably prove who initiated a transaction.

In their work on modernising payment services regulation and wider work on the development of a new retail payments infrastructure, HMT and regulators should consider how to future-proof

the revised regulatory landscape against this risk. This should involve investigating how to encourage payment providers to build adaptable systems capable of upgrading encryption standards without disrupting consumer services. Regulators should also consider how post-quantum readiness fits into the FCA's operational resilience expectations, while ensuring statutory liability rules continue to protect consumers from financial loss or unfair burdens of proof if standard encryption protocols are compromised by technological advances.

Ensuring payments resilience when digital networks fail. As the UK moves toward an increasingly cashless society, heavy reliance on continuous connectivity leaves the economy vulnerable to power grid disruptions, cellular network outages, or crashes of cloud computing. Without functional offline payment options, even a brief localised network outage has the potential to leave consumers unable to purchase essentials like food, medicine, or transport. In addition, if offline digital transactions synchronize incorrectly once connectivity is restored, consumers could face unexpected charges, delayed payments, or duplicate charges through no fault of their own. HM Treasury and regulators should explore the key safety, operational, and consumer protection standards required for the operation of offline payments during network outages. It may be that the Bank of England's work on offline payments for a Digital Pound can provide useful insights on this matter.

Crucially, this work must be paired with a firm commitment to maintaining access to cash. We welcome the positive steps already taken by the Government and the FCA to protect cash access. HMT should ensure these statutory cash protections are maintained and safeguarded as the digital payment framework is modernised. Physical cash is not only the ultimate backup for economic resilience when digital networks fail, but also a vital anchor for payment interoperability, ensuring no consumer is locked out of the economy by technical incompatibility or system outages.

Question 17: How can the Government ensure these reforms support an inclusive payments landscape?

To deliver a genuinely inclusive payments landscape under the Modernising Payments Regulation framework, HM Treasury must ensure that regulatory modernisation does not leave digitally or financially vulnerable consumers behind.

In our response to the Retail Payments Infrastructure Board (RPIB) consultation on the Design of the Future Retail Payments Infrastructure we observed that the advent of a new retail payments infrastructure presents a once-in-a-generation opportunity to build a system that works for everyone, including those currently excluded or underserved. We therefore argue that financial inclusion must be established as a standalone design principle for new retail payments infrastructure, backed by a clear regulatory mandate.

However, HMT can take action now as it considers reforms to the current regulation of payment services. In particular, there are several actions which we recommend, and which we highlighted in answer to Question 2:

- **Non-digital service baseline:** As payment infrastructure shifts to online and digital channels making use of biometrics and smartphones, we risk excluding those who cannot access these technologies. Legislation should include explicit duties requiring firms to maintain accessible, non-digital servicing channels (e.g. telephone or physical

branch access) for essential tasks, including dealing with suspected fraud and dispute resolution. As we note in our answer to Question 2, the FCA has recently reviewed payments firms' approaches to supporting consumers in vulnerable circumstances and warned that pure digital or transactional business models "amplify the potential for harm" due to limited human contact when issues arise, reinforcing the need for a right for customers escalate issues to a human where they are unable to resolve problems.

- **Delegated digital access framework:** The current legislative framework forces millions of vulnerable consumers to adopt high-risk workarounds, such as sharing banking passwords or PINs with carers, which leaves them open to abuse and voids fraud liability protections. Research conducted by Devon Fields Consultancy, and cited in the Consumer Vision for Payments report, highlights that more than 11 million 'financial helpers' across the UK regularly assist relatives, carers, or friends with managing day-to-day banking and payments yet frequently lack safe, formal tools to do so. The City of London Police, citing data from Report Fraud, has revealed that trusted family members, friends, carers, employees, or individuals entrusted to manage another person's finances or affairs stole £93.8 million through fraud by abuse of position during the 2025/26 financial year, with people aged 70 and over accounting for more than £51 million of those losses. Legislation should require PSPs to implement a secure, standardised digital delegation tool. This tool must allow account holders to grant trusted third parties (e.g. carers) flexible and granular permissions (e.g. 'pay energy bill of up to £100pcm") without requiring the sharing of full credentials or account control.
- **Baseline for payment purchase protections:** As new payment methods emerge, we are witnessing a dangerous 'protection gap' emerge. Current consumer purchase protection rights - such as those under Section 75 of the Consumer Credit Act or chargeback - are tied to specific payment methods, leaving consumers unknowingly unprotected when they use newer retail payment rails such as Open Banking account-to-account payments. Industry efforts to address this gap for what is commonly referred to as Pay By Bank have failed to deliver, despite this payment method becoming increasingly popular. We have little confidence that it will be satisfactorily resolved any time soon. Legislation should mandate that all digital payment transactions must incorporate a baseline dispute and refund standard. This would help to give consumers the confidence to try new and emerging digital payment methods, encouraging innovation and competition.

In addition, as reforms are made to areas such as SCA, HMT and FCA should seek to ensure that the move to a more outcomes-based approach delivers for all consumers, including those who may not have access to technologically sophisticated smartphones. When SCA was first introduced, Which? reported that some consumers experienced difficulties, and some banks initially failed to provide suitable alternatives. Lessons should be learned from this to ensure the flexibility offered by the move to an outcomes-based approach delivers for all consumers. This could include requiring the provision of non-digital authentication methods, ensuring all authentication interfaces comply with accessibility standards, and mandating standardised error messaging where authentication fails.

Question 18: What are the key risks which have emerged in the payments and electronic money sector over recent years?

There are a number of key risks that have emerged in the payments and electronic money sector over recent years. We suggest that many of these stem from three fundamental regulatory and structural failures:

- **Delays in extending regulation -** The delays inherent in updating legislation and extending the regulatory perimeter has created a lag between market innovation and consumer protection. Novel products like Buy Now, Pay Later (BNPL) rapidly grew outside the regulatory perimeter. Which? research shows this lag caused consumer detriment, leaving users exposed without standard protections, mandatory affordability checks, or access to the FOS.
- **Fragmented protection framework -** The proliferation of new payment rails and non-bank providers has created a multi-tiered, confusing protection landscape for consumers. Paying for the same item can result in drastically different rights depending on whether a transaction uses a credit card (Section 75), debit card (chargeback), or account-to-account payment, even where the experience for the consumer is virtually identical. Which? research demonstrates that consumers assume any payment carried out by an FCA-regulated financial firm carries protections but the reality is very different, and can mean that consumers do not receive the protection they expect.
- **Digital and financial exclusion -** As payment providers prioritise a digital-first approach, we are witnessing the rapid dismantling of physical payment infrastructure and accessible customer support channels. Which? tracking highlights the staggering scale of the decline of local bank branches which can isolate vulnerable, low-income, and digitally disengaged consumers. Without action to require universal access, large numbers of people face becoming marginalised or excluded.

Question 19: Would enhanced accountability of senior managers support efforts to manage financial crime risks in the payment services and electronic money sector? Would there be any risks to international competitiveness from this?
Question 20: Are there targeted amendments that could be made to current regulation which would tackle sector risks in a proportionate way?

Yes. Extending accountability of senior managers through the application of the Senior Managers & Certification Regime (SM&CR) to the payment services and electronic money sector is a vital step toward modernizing the regulatory framework and bringing the payments sector into line with the rest of the UK financial services industry. The FCA has repeatedly highlighted governance deficiencies in the sector, for example in its 2025 portfolio letter to payments firms, the FCA explicitly stated that *"weaknesses in governance, oversight and leadership are a root cause of many of the regulatory issues that they see in the payments portfolio."* Rapid commercial growth has frequently outpaced internal risk management, client fund safeguarding controls, and financial crime oversight. Seeking to act on these shortcomings, the FCA has proposed in its Perimeter Report that payments and e-money firms should be brought into scope of the SM&CR. We support this move.

Applying the SM&CR will directly target and improve how payments firms manage financial crime risks such as Anti-Money Laundering (AML) controls, Authorised Push Payment (APP) fraud prevention, and Money Laundering Reporting Officer (MLRO) oversight - by ensuring clear executive ownership, and holding senior leaders personally accountable for safeguarding and financial crime systems. The Bank of England found that across other sectors, the SM&CR has

proven highly effective in raising professional standards, driving individual accountability, and improving governance. Meanwhile, feedback from firms to the FCA confirmed that *"the overall view was that the SM&CR is a valuable regime, and that it is generally meeting its objectives"* and furthermore, *"many respondents said that SM&CR had the overall effect of improving governance, behaviours and culture within firms."*

Applying the regime to payment firms offers the same prospect: incentivising proactive board oversight, strengthening safeguards around client money, and reducing systemic risks like money laundering and fraud. The regulators are already undertaking reform to improve the efficiency and effectiveness of the regime. Such reform will help to reduce burdensome administrative elements, while the fact that the SM&CR applies proportionally based on a firm's size, operational complexity, and regulatory permissions should mitigate any concerns about adverse impacts on smaller firms.

Chapter 4 questions - Unlocking the future of Open Banking

Summary of our approach

We support the transition of Open Banking from a remedy imposed by the Competition and Markets Authority (CMA) to a permanent, statutory framework overseen by the FCA under the Data (Use and Access) Act 2025. Open Banking has the potential to increase retail competition, reduce card transaction fees for merchants, and help consumers manage household budgets. However, expanding Open Banking must not result in a net dilution of consumer safety, consent ownership, or financial redress.

Rather than answering every question individually, our response groups Questions 21-41 into four areas and focuses on core consumer priorities.

1: Consumer Protection and Sweeping (Q21, Q26, and Q31)
We support establishing a statutory right of access for Variable Recurring Payments (VRPs) (Q21). Expanding VRPs beyond basic self-sweeping into commercial retail use cases can provide an alternative to established recurring payment mechanisms like Direct Debits and Continuous Payment Authorities (CPAs). As Which? research highlights, the existing recurring payment mechanisms often fail to deliver the control consumers expect, driving a strong appetite for more visible, predictable, and flexible alternatives. However, VRPs will only secure consumer trust if:

- managing or cancelling a recurring payment instruction is as simple and frictionless as initiating one. Banking apps should feature consumer controls which allow for this via a prominent, standardized 'One-Click Revocation' mechanism.
- they offer similar levels of protection consumers rely on and expect to feature such as the Direct Debit Guarantee, and similar functionalities which are included in the Current Account Switch Service (CASS) automatic switching mechanism.

Furthermore, maintaining mandatory, fee-free sweeping functionality across all retail banks remains essential (Question 31). Automated "me-to-me" sweeping allows consumers to seamlessly transfer funds between their own accounts - and could potentially include instant-access cash savings and Cash ISAs should the definition of a payment account be

amended as per the suggestion in our response to Question 3 above. This serves as an effective tool for consumers to build savings buffers, optimise interest earned, and avoid overdraft charges.

Finally, in response to Question 26, foundational consumer protections and access rights should remain firmly anchored in secondary legislation. Core principles such as non-discriminatory access rules for Third Party Providers (TPPs) and basic user consent frameworks should remain preserved in statute rather than delegated entirely to commercial scheme rules or regulatory guidance.

2: Commercial pricing (Q22, Q23, Q33, Q34, and Q35)
Statutory APIs for basic Account Information Services (AIS) and standard Payment Initiation Services (PIS) should remain free of charge for TPPs (Question 22). Allowing banks to monetize basic compliance access would undermine competition from fintechs and restore incumbent bank dominance, defeating the original intention of Open Banking.

In relation to Questions 33 and 34, where banks are permitted to charge for advanced premium APIs or commercial VRP infrastructure, the FCA should be granted powers to intervene and enforce price caps, subject to Competition Act considerations. Without direct price intervention powers, incumbent banks could inflate transaction costs, which merchants are likely to pass on to consumers.

We oppose lifting prohibitions on individual bilateral contracts between major banks and TPPs (Questions 23 and 35). Allowing bilateral agreements would create a fragmented, tiered market where small fintech innovators may be priced out by dominant retail banks. Instead, we'd prefer to see a single, standardized, multilateral commercial scheme to ensure fair terms, open access, and robust consumer protections across the entire market.

3: Universal participation and Governance (Q28, Q29, Q30, Q32, Q36, and Q39)
The FCA must be granted direct powers to place requirements on ecosystem participants and compel all major retail banks to participate in commercial Open Banking schemes (Questions 28 and 29). Relying on voluntary bank participation would restrict coverage. This would frustrate the National Payment Vision's ambition that *"seamless account-to-account payments are developed as a ubiquitous payment method"*. It would also reduce the positive impacts of the 'network effect' and render account-to-account payments patchy and unreliable for both consumers and merchants.

Part of the CMA Order requires in-scope banks to release 'product' and 'reference' information via Open Banking APIs. (Question 30) This includes information relating to financial products and pricing covered by the Order, physical infrastructure (e.g. for bank branches), quality of service and uptime. We are not aware of published data about usage levels of such APIs but note that Which? has made use of API data on accessibility, finding that *"when we looked at the public data supplied by the nine largest UK banks via application programming interfaces (APIs) we found that most have published unreliable information about accessibility*".

Other consumer-facing services may make use of the information, for example price comparison sites may use real-time product APIs to maintain up-to-date comparison tables for certain products, budgeting apps can make use of market reference data to recommend

cheaper overdrafts or higher-reward current accounts, and location / navigation services can pull data from APIs to display accurate branch hours and accessibility features.

Such use cases mean that it would be beneficial to maintain a requirement on banks to publish accurate and up to date 'product' and 'reference' information via Open Banking APIs, though consideration should be given to extend the obligation beyond the CMA9 banks.

Finally, we would observe that it appears odd for HMT to consider stopping or limiting access to data that serves a useful purpose, at a time when the general trend is to move towards the release of more data. Indeed, we would note that stopping the provision of such data could unhelpfully undermine potential moves to facilitate use of agentic AI which will rely on access to more, not less, high quality data so agents can make recommendations or even execute product or provider switches.

Regarding Questions 32, 36, and 39, the Future Entity that is designated to oversee technical Open Banking standards should operate under direct FCA supervisory oversight, with equal representation for consumer advocates, fintechs, and merchants. The Future Entity should also collaborate with smart data schemes in other sectors to ensure design consistency and interoperability. Coordinated efforts will maximize consumer benefits, especially from schemes operating across multiple sectors. Partnering with the Department for Business, Innovation, Science and Trade (BIST) on the Smart Data Guidebook, as well as with other sector oversight bodies and regulators, will help align the smart data ecosystem.

In line with Which?'s policy paper 'Building consumer trust in Smart Data', the oversight framework for the Future Entity and commercial Open Banking schemes must be anchored on a mandatory Smart Data Trust Framework based on three core pillars:

- **Governance:** Clear roles and responsibilities, transparent oversight, robust liability rules, the monitoring of consumer outcomes and accessible dispute resolution to maintain consumer confidence.
- **Protection:** Uncompromising cybersecurity, strict data minimization, and privacy standards to ensure fundamental consumer rights are never diluted.
- **Scalability & Inclusion:** Inclusive-by-design requirements, standardized operational definitions, and common language to ensure all consumers, including vulnerable users, can safely navigate smart data services.
- **Scheme must address the needs of vulnerable consumers**.
- **Government should take a coordinating role in the development of smart data**.

Finally, Open Banking must also address the needs of vulnerable consumers. Research by the Social Market Foundation (funded by Which?) found that vulnerable consumers could benefit most from smart data schemes. But if those schemes are perceived as risky, the vulnerable people who stand to gain the greatest benefits may be the least likely to participate.

4: Objectives, Enforcement, and Data Ethics (Q25, Q27, Q37, Q38, Q40, and Q41)
Addressing Questions 25 and 27, the statutory definition of a 'payment account' should be modernized to encompass instant-access cash savings and Cash ISAs (as we set out in our answer to Question 3). Alongside updated definitions, the FCA must enforce strict operational performance SLAs (e.g. 99.9% API uptime) so consumers and retailers can rely on these payments and they can be viewed as a genuine alternative payment method. Where operational

failures occur and disrupt retail payments, the FCA should have powers to levy financial penalties.

We strongly support mirroring FSMA monitoring and enforcement powers, providing the FCA with comprehensive investigative tools, compliance notices, and real-time technical auditing capabilities to prevent deliberate API performance throttling (Questions 37 and 38).

However, while mirroring FSMA objectives is appropriate, the FCA's primary statutory duty to protect consumers must take precedence over secondary growth or international competitiveness duties (Question 40).

We are not convinced that adding an additional objective to reflect the broader data-focused aims of the Data (Use and Access) Act 2025 (DUAA) and to support its approach to regulating Open Banking is necessary or required (Question 41) provided that the primacy of the consumer protection duty remains. The FCA already has a range of objectives, and though there is a trend to want to add ever more additional objectives, we are concerned that this may complicate the regulator's decision-making process.

However, if the FCA is to be given an additional objective which reflects the broader data-focused aims of DUAA, it should be grounded in what consumers need and expect. As highlighted in 'Building consumer trust in Smart Data', regulatory oversight and the FCA's statutory objectives must explicitly guard against data exploitation, dark patterns, predatory credit scoring/pricing, and aggressive profiling of vulnerable consumers. Open Banking and Smart Data governance must ensure data access is strictly purpose-bound, transparent, and used solely to empower consumers rather than extract unfair commercial value at their expense.

Question 42: Are there any other areas of feedback on issues raised in this consultation?

No.

About Which?

Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.

For more information contact:
Tony Herbert, Senior Policy Adviser
tony.herbert@which.co.uk
October 2026